Université de Bordeaux — L3 Math, Info, Math-Info
Collège Sciences et Technologies

Année Universitaire 2013-2014
Devoir Surveillé
Parcours : IN601, MA601, MA603 **UE :** N1MA6W31
Épreuve : Cryptographie et Arithmétique
Date : 17 Mars 2014 **Heure :** 11h00 **Durée :** 1h30
Documents : Aucun document autorisé
Épreuve de M. Cerri

L'usage de la calculatrice est autorisé.

Exercice 1 [Chiffrement affine]

Soient $n \geq 2$ un entier. L'ensemble des messages clairs possibles est $\mathbb{Z}/n\mathbb{Z}$. Pour simplifier les notations on identifie les éléments de $\mathbb{Z}/n\mathbb{Z}$ avec les entiers $0, 1, \ldots, n-1$. Le système de chiffrement utilisé par Alice et Bob est un système symétrique. Leur secret commun est un couple (a, b) d'entiers vérifiant $0 \leq a, b \leq n-1$. Alice désire envoyer le message m à Bob. Pour cela elle calcule le chiffré $c = am + b \bmod n$ qu'elle communique à Bob.
1. Montrer que $f : m \mapsto am + b$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même si et seulement si a est inversible modulo n.
On suppose désormais que cette condition est vérifiée.
2. Quel calcul Bob effectue-t-il à partir de c pour retrouver m ?
3. Application : $n = 123$, $a = 5$, $b = 13$. Bob reçoit le chiffré $c = 76$. Retrouver m.
4. Attaque d'Oscar à couples clairs-chiffrés connus. Oscar sait que $n = 123$ et connaît les deux couples (m, c) suivants : $(3, 56)$, $(17, 25)$. Montrer qu'Oscar peut retrouver la clé secrète (a, b) d'Alice et la calculer.

Exercice 2 [Théorème Chinois]

Résoudre dans $\mathbb{Z}$ le système

$$\begin{cases} 2x & \equiv & 3 \bmod 15 \\ 3x & \equiv & 1 \bmod 16 \\ 4x & \equiv & 8 \bmod 14 \end{cases}$$

Exercice 3 [Indicateur d'Euler]

Les deux questions sont indépendantes. Dans ce qui suit ϕ désigne l'indicateur d'Euler.
1. Soit $n \geq 2$ un entier. En remarquant que si $k \geq 1$ est un entier tel que $\text{pgcd}(k, n) = 1$ alors $\text{pgcd}(n-k, n) = 1$, montrer que

$$\sum_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} k = \frac{1}{2} n\phi(n).$$

2. Montrer que si m et n sont deux entiers ≥ 1 et si $d = \text{pgcd}(m, n)$, on a

$$\phi(d)\phi(mn) = d\phi(m)\phi(n).$$

Exercice 4 [RSA]

Bob et Alice utilisent RSA. La clé publique de Bob est (N, e) où $N = 45743$ est le produit de deux premiers distincts p et q.

1. Sachant que $\phi(N) = 45288$, déterminer p et q.

2. Bob choisit $e = 155$. Montrer que c'est un choix correct. Quel est l'exposant de déchiffrement d que Bob va utiliser ?

3. Variante de RSA. Soient trois premiers distincts p, q, r et $N = pqr$. La clé publique de Bob est (N, e) où e est inversible modulo $\phi(N)$, d'inverse d modulo $\phi(N)$. Alice chiffre le clair $m \in \mathbb{Z}/N\mathbb{Z}$ par $c = m^e \bmod N$. Bob déchiffre c en calculant $m' = c^d \bmod N$. Prouver que cette procédure de déchiffrement est correcte, i.e. que $m' = m$. On pourra montrer que $m' = m$ modulo p, q et r et conclure.